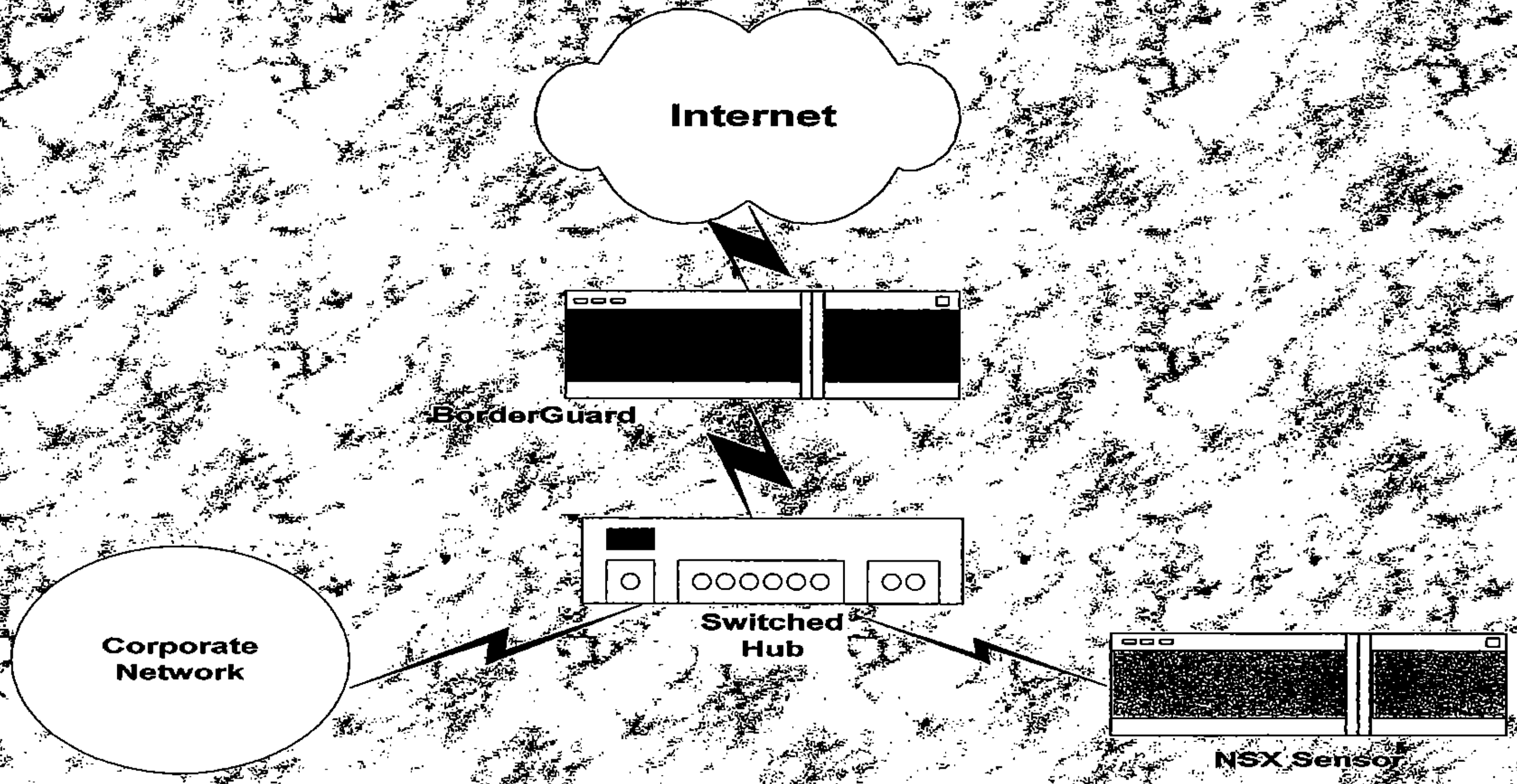
WheelGroup corporation

Install on a Switched Ethernet Network



WheelGroup corporation

NetRanger Director Setup Options

Two considerations when setting up a Director

- Place the Director close to the individuals responsible for monitoring the networks
- There must be a path between the NSX and the Director for the alarm and management functions to work properly

WheelGroup corporation

Gather Network and Security Information

- BorderGuard/Passport IP Addresses (One for each interface)
- NSX IP Address
- Director IP Address
- Internal Web Server Address
- Internal DNS Server Address
- Internal FTP Server Address

WheelGroup corporation

Internet Control Message Protocol (ICMP)

- Allows routers and hosts to send error and control messages to other routers and hosts.
- Most frequent use is the "ping" command
- Map out allowable ICMP messages

WheelGroup corporation

Example ICMP Messages

- Echo Request
- Echo Reply
- Destination Unreachable
- Address Mask Request
- Address Mask Reply
- Redirect (change a route)
- Source Quench

WheelGroup corporation

Transmission Control Protocol

- Most used transport protocol used on Ethernet and Internet
- Connection is established every time a TCP service is used
- Certain incoming services can be blocked while allowing outgoing traffic
- Map out TCP Allowed Services

WheelGroup corporation

Example TCP services

- FTP Reply (Source Port 20)
- FTP (Port 21)
- Telnet (Port 23)
- SMTP (Mail, Port 25)
- DNS (Port 53)
- WWW (Port 80)
- Printer (Port 515)

WheelGroup corporation

User Datagram Protocol (UDP)

- Very few UDP Services should be allowed between your network and untrusted sites
- UDP is Connectionless which makes it impossible to distinguish between session initiation and general session data

WheelGroup corporation

Example UPD Services

- DNS (Port 53)
- TFTP (Port 69)
- RPC (Port 111)
- NTP (Port 123)
- Netbios (Ports 137-139)
- SNMP (Ports 161,162)
- RIP (Port 520)

WheelGroup corporation

Traditional Security Basics

WheelGroup corporation

Overview

- Traditional Security Measures
- Computer Emergency Response Teams (CERTs)
- Firewalls
- Encryption
- Next Generation Security

WheelGroup corporation

Traditional Security Measures

- Host based
  - Passwords (Standard and Alternative)
  - Security patches
  - Audit trails
- Managed by system administrator
  - Reliant upon individual initiative
  - First responsibility is functioning network

WheelGroup corporation

Computer Emergency Response Teams (CERTs)

- Distribute advisories notifying administrators of security holes
- Respond to hacking incidents
- Work with vendors to produce security patches and notify computer community

WheelGroup corporation

CERT Problems

- Reactive instead of proactive
- Unorganized solutions to problems
  - Flat file system of released advisories
  - No customization to customer's needs
- Originally not a commercial organization
- Requires administrators to constantly fix buggy systems
- High administrative overhead

WheelGroup corporation

Firewalls

- Significant improvement over host-based security
- Network based
- Filtering Routers vs Application Gateways
- Improved Audit Capabilities